

RESPONDER FOR COMMUNICATION AND COMMUNICATION SYSTEM USING IT

Publication number: JP2000252854

Publication date: 2000-09-14

Inventor: HIKITA JUNICHI; IKUTO YOSHIHIRO; TAGUCHI HARUO

Applicant: ROHM CO LTD

Classification:




- international: *G06K17/00; G06K19/073; G07F7/10; G09C1/00; H04B1/59; H04B5/02; H04L9/32; G06K17/00; G06K19/073; G07F7/10; G09C1/00; H04B1/59; H04B5/02; H04L9/32; (IPC1-7): H04B1/59; G06K17/00; G09C1/00; H04B5/02; H04L9/32*

- European: H04L9/32; G07F7/10D10M2

Application number: JP19990049678 19990226

Priority number(s): JP19990049678 19990226

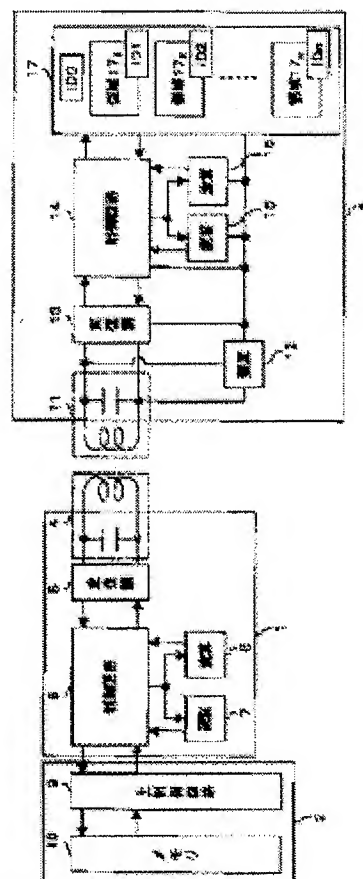
Also published as:

 US6747546 (B1)
 GB2350021 (A)
 AU768579B (B2)

Report a data error here

Abstract of JP2000252854

PROBLEM TO BE SOLVED: To provide a communication responder, where an encryption key for making a memory area available is set to each IC card, to enhance security and a communication system using it. **SOLUTION:** An IC card 3 stores an ID ID0 for identification of the IC card 3 in a memory. Further, ID ID1-IDn are given to each of memory areas 171-17n allocated to each provider managing a reader/writer 1 so as to avoid illegal use during communication. Since the provider using the memory areas 171-17n for each IC card provides the ID ID1-IDn, the number of the IDs differ in respective IC cards.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-252854

(P2000-252854A)

(43)公開日 平成12年9月14日(2000.9.14)

(51)Int.Cl. ⁷	識別記号	F I	チーマート*(参考)
H 0 4 B 1/59		H 0 4 B 1/59	5 B 0 5 8
G 0 6 K 17/00		G 0 6 K 17/00	F 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 A 5 K 0 1 2
H 0 4 B 5/02		H 0 4 B 5/02	9 A 0 0 1
H 0 4 L 9/32		H 0 4 L 9/00	6 7 1
審査請求 未請求 請求項の数6 O L (全 13 頁)			

(21)出願番号 特願平11-49678

(22)出願日 平成11年2月26日(1999.2.26)

(71)出願人 000116024

ローム株式会社

京都府京都市右京区西院溝崎町21番地

(72)発明者 正田 純一

京都市右京区西院溝崎町21番地 ローム株式会社内

(72)発明者 生藤 義弘

京都市右京区西院溝崎町21番地 ローム株式会社内

(74)代理人 100085501

弁理士 佐野 静夫

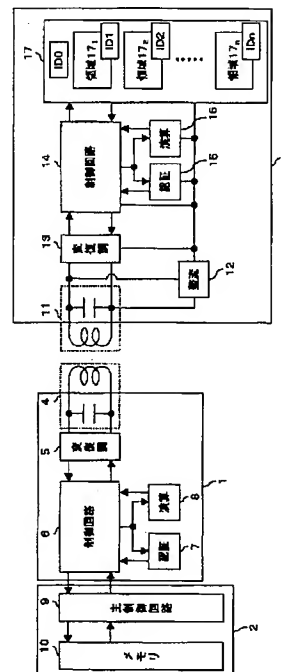
最終頁に続く

(54)【発明の名称】 通信用応答器及びこれを用いた通信システム

(57)【要約】

【課題】本発明は、メモリ領域を使用可能にするための暗号鍵を、ICカード毎に設定し、更に安全性の高い通信用応答器及びこれを用いた通信システムを提供することを目的とする。

【解決手段】ICカード3は個々に識別するためのID ID0をメモリ内に記憶している上に、リーダ・ライタ1を管理するプロバイダ毎に振り分けられたメモリ領域17₁~17_nのそれぞれに、通信時に不正な使用が行われないように、ID ID1~IDnが与えられる。このID1~IDnは、ICカード毎にメモリ領域17₁~17_nを使用するプロバイダが提供するので、IDの番号は、個々のICカード間で異なる。



【特許請求の範囲】

【請求項1】 管理元が異なる複数の質問器と個々に通信を行うことが可能であるとともに、前記質問器との通信において使用される情報が記憶される複数の記憶領域を有する通信用応答器において、

該応答器と前記質問器が通信を行う際に使用する特定の記憶領域のみを使用可能とする該応答器固有の鍵信号を、それぞれの記憶領域に対して記憶し、

前記質問器と通信を行う際に、前記質問器から送信される鍵信号を照合して前記応答器に記憶された鍵信号と一致したとき、前記特定の記憶領域のみを使用して前記質問器と通信可能となることを特徴とする通信用応答器。

【請求項2】 前記質問器に送信する通信の許可を求めるための信号を生成する認証手段を有することを特徴とする請求項1に記載の通信用応答器。

【請求項3】 前記質問器から通信の許可を求めてきた信号を検知し、該信号によって前記質問器が適正なものか否かを判別するとともに、前記質問器が適正であるとき通信を許可する認証手段を有することを特徴とする請求項1に記載の通信用応答器。

【請求項4】 前記質問器から送信される命令信号に付加された通信の許可を求める信号に特定の演算処理を施して前記質問器に送信する応答信号に付加する演算手段と、前記命令信号に付加された通信の許可を求める信号によって前記質問器が適正であるか否かを判別する認証手段を有するとともに、

前記演算手段によって前記特定の演算処理が施されるとともに前記応答信号に付加された信号が、前記質問器において、前記応答器が適正であるか否かを判別するための信号であることを特徴とする請求項1に記載の通信用応答器。

【請求項5】 前記記憶領域の少なくとも1領域が、前記質問器と通信を行う際に該記憶領域が使用されるとき、前記質問器から与えられる度数変更命令に応じて、該記憶領域内に記憶されている度数を変更する度数記憶部材によって構成されることを特徴とする請求項1～4のいずれかに記載の通信用応答器。

【請求項6】 請求項1～5のいずれかに記載の応答器と前記質問器が非接触で通信を行うことを特徴とする非接触通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、高周波タグやICカードといった通信用応答器及びこれを用いた通信システムに関するもので、特に、複数のプロバイダの質問器との通信に応じて使用される複数の記憶領域を有する通信用応答器及びこれを用いた通信システムに関する。

【0002】

【従来の技術】近年、応答器として使用されるICカード1枚で、多数のプロバイダがそれぞれに管理する複数

種類のリーダー・ライター（質問器）と通信が可能となるような通信システムが提供されている。このような通信システムを実現するために、前記ICカード内に設けられたメモリを区分して、多数のプロバイダがそれぞれに管理する前記リーダー・ライターとの通信のやり取りを行う際にデータを格納するためのメモリとして使用されるように、複数のメモリ領域が前記プロバイダに応じて割り当てられている。このように、1枚のICカードで多数のプロバイダがそれぞれに管理する前記リーダー・ライターと通信を行うことができるので、通信を行う際、現在通信を行っているリーダー・ライターを管理するプロバイダに割り当てられた特定のメモリ領域のみを使用可能とするとともに、それ以外のメモリ領域を使用不可能とする必要がある。

【0003】そのため、ICカードには、それぞれのメモリ領域に割り当てられたプロバイダの管理するリーダー・ライターと通信を行うときのみに使用可能とするための暗号鍵が複数記憶されている。そして、この暗号鍵を使用して、ICカード及びリーダー・ライター間で相互認証処理が行われる。このような相互認証処理を行う非接触通信システムが、特開平10-327142号公報に提示されている。

【0004】特開平10-327142号公報に提示される通信システムでは、図11のように、ICカード内に記憶されたそれぞれのメモリ領域（エリア）を使用可能にするための前記暗号鍵は、プロバイダ毎に決定される。更に、この暗号鍵によって認証されたリーダー・ライターがアクセスを要求するメモリ領域を判別することができる。一方、リーダー・ライター側では、前記暗号鍵によって、ICカードが適正なものか否かを判断することができるが、個々のICカードを判別することができない。そのため、リーダー・ライターがICカードを判別するために、予めICカードそれぞれに固有のID番号を記憶させる。

【0005】

【発明が決しようとする課題】しかしながら、特開平10-327142号公報で提供されるICカード内のメモリ領域を使用可能にするための暗号鍵は、プロバイダ毎に設定されたものであり、ICカード固有の暗号鍵でない。そこで、本発明は、メモリ領域を使用可能にするための暗号鍵を、ICカード毎に設定し、更に安全性の高い通信用応答器及びこれを用いた通信システムを提供することを目的とする。

【0006】又、特開平10-327142号公報で提供されるICカード内に記憶されるID番号は生産時に発行されるものなので、このID番号をICカードに記憶させると同時に、各プロバイダも同時にそのID番号を認知させる必要がある。よって、ICカードを生産する毎に、各プロバイダにそのID番号を認知させなければならないので、この通信システムにおける管理が煩雑

となる。

【0007】

【課題を解決するための手段】請求項1に記載の通信用応答器は、管理元が異なる複数の質問器と個々に通信を行うことが可能であるとともに、前記質問器との通信において使用される情報が記憶される複数の記憶領域を有する通信用応答器において、該応答器と前記質問器が通信を行う際に使用する特定の記憶領域のみを使用可能とする該応答器固有の鍵信号を、それぞれの記憶領域に対して記憶し、前記質問器と通信を行う際に、前記質問器から送信される鍵信号を照合して前記応答器に記憶された鍵信号と一致したとき、前記特定の記憶領域のみを使用して前記質問器と通信可能となることを特徴とする。

【0008】このような通信用応答器において、該応答器と通信可能な質問器の管理元であるプロバイダが、該応答器及び該質問器を使用して通信を行う際に使用する記憶領域の鍵信号を、応答器毎に設定する。このように鍵信号が設定された応答器が、前記質問器と通信を行おうとしたとき、質問器側で応答器を個別に判断することができる。

【0009】請求項2に記載の通信用応答器は、請求項1に記載の通信用応答器において、前記質問器に送信する通信の許可を求めるための信号を生成する認証手段を有することを特徴とする。

【0010】請求項3に記載の通信用応答器は、請求項1に記載の通信用応答器において、前記質問器から通信の許可を求めてきた信号を検知し、該信号によって前記質問器が適正なものの否かを判別するとともに、前記質問器が適正であるとき通信を許可する認証手段を有することを特徴とする。

【0011】請求項4に記載の通信用応答器は、請求項1に記載の通信用応答器において、前記質問器から送信される命令信号に付加された通信の許可を求める信号に特定の演算処理を施して前記質問器に送信する応答信号に付加する演算手段と、前記命令信号に付加された通信の許可を求める信号によって前記質問器が適正であるか否かを判別する認証手段を有するとともに、前記演算手段によって前記特定の演算処理が施されるとともに前記応答信号に付加された信号が、前記質問器において、前記応答器が適正であるか否かを判別するための信号であることを特徴とする。

【0012】請求項5に記載の通信用応答器は、請求項1～4のいずれかに記載の通信用応答器において、前記記憶領域の少なくとも1領域が、前記質問器と通信を行う際に該記憶領域が使用されるとき、前記質問器から与えられる度数変更命令に応じて、該記憶領域内に記憶されている度数を変更する度数記憶部材によって構成されることを特徴とする。

【0013】請求項6に記載の通信システムは、請求項1～5のいずれかに記載の応答器と前記質問器が非接触

で通信を行うことを特徴とする。

【0014】

【発明の実施の形態】本発明の第1の実施形態について、図面を参照して説明する。図1は、本実施形態における通信システムの構成を示すブロック図である。図2は、本実施形態における通信システムの動作を示すタイムチャートである。尚、以下、NGとは、認証を行ったとき認証する相手が不適正であることを、OKとは認証を行ったとき認証する相手が適正であることを意味する。

【0015】図1に示す通信システムは、質問器となるリーダー・ライター1及びコントローラ2と、応答器となるICカード3とを有する。このような通信システムにおいて、リーダー・ライター1は、ICカード3と信号の送受信を行う同調回路4と、同調回路4で受信した応答信号を復調するとともに制御回路6より送出される命令信号を変調する変復調回路5と、命令信号を生成する制御回路6と、受信した応答信号に付加された認証信号が制御回路6より送出されるとともに該認証信号によってICカード3の認証を行う認証回路7と、受信した応答信号に付加された認証信号が制御回路6より送出されるとともに該認証信号に所定の演算処理f1()を行う演算回路8とから構成される。このようなリーダー・ライター1を制御するとともに通信を行うコントローラ2は、リーダー・ライター1の制御回路6と信号のやり取りをするとともにリーダー・ライター1の制御を行う主制御回路9と、ICカード3の所有者のID及び所有者に関する情報が記憶されたメモリ10とを有する。

【0016】又、ICカード3は、リーダー・ライター1と信号の送受信を行う同調回路11と、同調回路11で同調した信号を整流することによってICカード3の各ブロックに供給する電源電圧を生成する整流回路12と、同調回路11で受信した命令信号を復調するとともに制御回路14より送出される応答信号を変調する変復調回路13と、応答信号を生成する制御回路14と、受信した命令信号に付加された認証信号が制御回路14より送出されるとともに該認証信号によってリーダー・ライター1の認証を行う認証回路15と、受信した命令信号に付加された認証信号が制御回路14より送出されるとともに該認証信号に所定の演算処理f2()を行う演算回路16と、所有者の個人情報及びIDが記憶されるメモリ17とから構成される。

【0017】更に、このような構成のICカード3は、複数のプロバイダがそれぞれ管理するリーダー・ライターと通信可能であり、メモリ17内において、それぞれのプロバイダに、アクセスする領域17₁～17_nが振り分けられている。即ち、図3(a)のように、プロバイダA1の管理するリーダー・ライター1₁がICカード3と通信可能となったとき、その通信時にICカード3内のメモリ領域17₁の読み出し又は書き込みが行われ、又、図

3(b)のように、プロバイダA2の管理するリーダ・ライタ1₂がICカード3と通信可能となったとき、その通信時にICカード3内の別の領域となるメモリ領域17₂の読み出し又は書き込みが行われる。

【0018】又、メモリ領域17₁~17_nにアクセスするためのID番号(メモリIDとする。)ID1~ID_nと、プロバイダ側が個々のICカード3を認識するためのID番号(ユーザーIDとする。)ID0がメモリ17内に記憶されている。このID番号ID0~ID_nは、個々のICカード3によって設定されるもので、ユーザーID ID0は、生産時に生産者によって設定され、又、メモリID ID1~ID_nは、各プロバイダによって設定される。即ち、図4のように、ICカード3₁のメモリ17-1内に記憶するID番号をそれぞれID0₁及びID1₁~ID_{n1}とすると、ICカード3₂のメモリ17-2内に記憶するID番号はそれぞれID0₂及びID1₂~ID_{n2}となる。

【0019】更に、図4のように、プロバイダAが、ICカード3₁と通信する際はメモリ領域17₁-1を、ICカード3₂と通信する際はメモリ領域17₁-2を使用するとする。このとき、図5のように、プロバイダAが管理するコントローラ2のメモリ10は、ICカード3₁のユーザーID ID0₁とメモリ領域17₁-1のメモリID ID1₁とICカード3₁のユーザー情報とを、又、ICカード3₂のユーザーID ID0₂とメモリ領域17₁-2のメモリID ID1₂とICカード3₂のユーザー情報とを、それぞれ対応させて記憶している。

【0020】このような通信システムにおいて、図2のように、リーダ・ライタ1からある一定の期間毎に、ICカード3が認証動作を行うための認証信号(ローリングコード)Rcaが制御回路6で付加された命令信号Caを生成し(STEP1)、この命令信号Caを変復調回路5で変調して同調回路4よりICカード3へ送信する(STEP2)。このとき命令信号Caに付加する認証信号Rcaは、任意の信号で、演算回路8で演算f1()を施した信号でない。

【0021】ICカード3が同調回路11でこの命令信号Caを受信すると、整流回路12で電源電圧を生成するとともに、変復調回路13で復調し制御回路14に送出する。制御回路14では、命令信号Caより認証信号Rcaを検知して、この認証信号Rcaがリーダ・ライタ1内で演算f1()が施された信号であるか否かを判別するために認証回路15に認証信号Rcaを送出する(STEP3)。今、この認証信号Rcaは演算f1()が施された信号でないので、認証結果はNGとなり、ICカード3はリーダ・ライタ1を認証しない(STEP4)。

【0022】又、このとき同時に、制御回路14で検知された認証信号Rcaを演算回路16に送出して演算f

2()を施す(STEP5)。このように演算回路16で演算f2()を施した信号f2(Rca)を認証信号Rcbとして制御回路14に送出し、リーダ・ライタ1に送信する応答信号Raに付加する。又、制御回路14では、この応答信号Raに、メモリ17内に記憶されているユーザーID ID0の情報を付加する(STEP6)。このように生成された応答信号Raは、変復調回路13で変調され同調回路11よりリーダ・ライタ1に送信される(STEP7)。

【0023】リーダ・ライタ1がこの応答信号Raを同調回路4より受け、変復調回路5で復調した後、制御回路6に送出する。制御回路6では、応答信号Raより認証信号Rcb及びユーザーID ID0を検知して(STEP8)、この認証信号RcbがICカード3内で演算f2()が施された信号であるか否かを判別するために認証回路7に認証信号Rcbを送出する。今、この認証信号Rcb=f2(Rca)は演算f2()が施された信号であるので、リーダ・ライタ1はICカード3を認証する(STEP9)。

【0024】このとき、認証結果がNGの場合、コントローラ2との通信は行われず、制御回路6で検知された認証信号Rcbを演算回路8に送出し、演算回路8で演算f1()を施す。このように認証信号Rcbに演算f1()を施した信号f1(Rcb)を認証信号Rccとして制御回路6に送出する(STEP10)。又、認証結果がOKとなると、制御回路6で検知したユーザーID ID0をコントローラ2の主制御回路9に送出し(ステップ11)、このユーザーID ID0に対応させてメモリ10内に記憶したICカード3のメモリ領域17₁を使用可能にするためのメモリID ID1を読み出す(STEP12)。そして、コントローラ2は、メモリ10より読み出したメモリID ID1を、主制御回路9からリーダ・ライタ1の制御回路6に送出する(STEP13)。

【0025】今、制御回路6において、認証回路7の認証結果がOKであれば、メモリID ID1、認証信号Rcc及びメモリ領域17₁を使用することを示す信号を付加した命令信号Cbを、又、認証回路7の認証結果がNGのときもしくはメモリ10内にユーザーID ID0が無いときは、認証信号Rccを付加した命令信号Cb'を変復調回路5に送出する(STEP14)。このようにして制御回路6より送出された命令信号Cb、Cb'を、変復調回路5で変調するとともに、同調回路4より送信する(STEP15)。

【0026】今、ICカード3の同調回路11で命令信号Cbを受信すると、整流回路12で電源電圧を生成するとともに、変復調回路13で復調し制御回路14に送出する。制御回路14では、命令信号Cbより認証信号Rcc及びメモリID ID1を検知するとともに、リーダ・ライタ1が使用するメモリ領域が領域17₁であ

ることを認識する (STEP 16)。そして、認証信号 Rcc がリーダー・ライター 1 内で演算 $f1()$ が施された信号であるか否かを判別するために認証回路 15 に認証信号 Rcc を送出する。尚、図 2 のタイムチャートには表記していないが、IC カード 3 が命令信号 Cb' を受信すると、リーダー・ライター 1、コントローラ 2、及び IC カード 3 において STEP 3 以降の動作を繰り返す。今、命令信号 Cb を受信したものであるとして、認証回路 15 で認証信号 Rcc によってリーダー・ライター 1 が適正か否かを認証する (STEP 17)。

【0027】このとき、認証結果が OK の場合、メモリ 17 内のメモリ領域 17_1 のメモリ ID と比較して、制御回路 14 にてリーダー・ライター 1 から送信されたメモリ ID が一致するか否かを判断し (STEP 18)、一致すれば STEP 20 に移行し、一致しなければ STEP 19 に移行する。又、STEP 17 で認証結果が NG となるとき、又は、STEP 18 でメモリ ID が不一致であるとき、制御回路 14 で検知された認証信号 Rcc を演算回路 16 に送出し、演算回路 16 で演算 $f2()$ を施す。このように認証信号 Rcc に演算 $f2()$ を施した信号 $f2(Rcc)$ を認証信号 Rcd として制御回路 14 に送出し (STEP 19)、STEP 20 に移行する。

【0028】STEP 18 又は STEP 19 のような処理動作が終了し STEP 20 に移行すると、認証結果が OK のときは通信可能であることをリーダー・ライター 1 に伝えるための応答信号 Rb を、認証結果が NG のときは認証信号 Rcd 及びユーザー ID $ID0$ を付加した応答信号 Rb' を制御回路 14 で生成して変復調回路 13 に送出する。今、認証信号 $Rcc = f1(Rcb)$ で且つ、リーダー・ライター 1 から送信されるメモリ ID は $ID1$ でありメモリ領域 17_1 のメモリ ID と一致するので、STEP 20 では、通信可能であることをリーダー・ライター 1 に伝えるための応答信号 Rb を生成する。このように応答信号 Rb 、 Rb' が変復調回路 13 に送出されると、それぞれ変調されて同調回路 11 より送信される (STEP 21)。

【0029】今、リーダー・ライター 1 の同調回路 4 で応答信号 Rb を受信すると、変復調回路 5 で復調し制御回路 6 に送出する。制御回路 6 では、応答信号 Rb より IC カード 3 内のメモリ領域 17_1 が開放され、通信可能となったことを認識する (STEP 22)。尚、図 2 のタイムチャートには表記していないが、リーダー・ライター 1 が応答信号 Rb' を受信すると、リーダー・ライター 1、コントローラ 2、及び IC カード 3 において STEP 8 以降の動作を繰り返す。

【0030】今、応答信号 Rb を受信したものであるとして、制御回路 6 よりコントローラ 2 の主制御回路 9 に IC カード 3 と通信可能であることを認識させる (STEP 23)。コントローラ 2 が IC カード 3 と通信可

能であることを認識すると、リーダー・ライター 1 を介して IC カード 3 と相互に通信を行い、この通信を行う際に IC カード 3 のメモリ領域 17_1 のデータの読み出し又は書き込みを行う (STEP 24)。

【0031】本発明の第 2 の実施形態について、図面を参照して説明する。図 6 は、本実施形態における通信システムの構成を示すブロック図である。図 7 は、本実施形態における通信システムの動作を示すタイムチャートである。尚、本実施形態の通信システムにおいて、図 6 に示すリーダー・ライター及びコントローラの内部構造は、図 1 の通信システム内におけるリーダー・ライター 1 及びコントローラ 2 の内部構造と同様のものとする。又、図 6 の IC カードを構成するブロックにおいて、図 1 の通信システム内における IC カード 3 を構成するブロックと同様のものは、同じ記号を付してその詳細な説明は省略する。

【0032】図 6 に示す IC カード 31 は、領域 $18_1 \sim 18_n$ に分割されたメモリ 18 と、同調回路 11 と、整流回路 12 と、変復調回路 13 と、制御回路 14 と、認証回路 15 と、演算回路 16 とを有し、又、第 1 の実施形態における IC カード 3 と同様、複数のプロバイダがそれぞれ管理するリーダー・ライターと通信可能であり、メモリ 18 内において、それぞれのプロバイダに、アクセスする領域 $18_1 \sim 18_n$ が振り分けられている。

【0033】又、メモリ領域 $18_1 \sim 18_n$ は、プロバイダ側が個々の IC カード 3 を認識するための ID 番号 (認識 ID とする。) $ID1a \sim IDna$ と、アクセスするための ID 番号 (メモリ ID とする。) $ID1b \sim IDnb$ とを有し、この認識 ID $ID1a \sim IDna$ 及びメモリ ID $ID1b \sim IDnb$ がメモリ 18 内に記憶されている。この認識 ID $ID1a \sim IDna$ 及びメモリ ID $ID1b \sim IDnb$ は、個々の IC カード 3 によって設定されるもので、生産後に各プロバイダにより設定される。

【0034】更に、図 8 のように、プロバイダ B が、IC カード 31 と通信する際はメモリ $18-1$ の内、領域 18_1-1 を、IC カード 31 と通信する際はメモリ $18-2$ の内、領域 18_1-2 を使用するとする。このとき、図 9 のように、コントローラ 2 のメモリ 10 は、IC カード 31 の認識 ID $ID1a-1$ とメモリ ID $ID1b-1$ とを、又、IC カード 31 のユーザー ID $ID1a-2$ とメモリ ID $ID1b-2$ とを、それぞれ対応させて記憶している。

【0035】このような通信システムの動作について、図 7 を使用して説明する。尚、図 2 と同様の動作は、同様であることを示しその詳細な説明は省略する。まず、リーダー・ライター 1 において、図 2 の STEP 1 及び STEP 2 と同様の処理を STEP 1a 及び STEP 2a で行い、認証信号 $Rc1$ を付加した命令信号を $C1$ を IC カード 31 に送信する。又、このとき、命令信号 $C1$ に

は、メモリ領域18₁へのアクセスを希望していることを示す信号も付加されている。

【0036】ICカード31が同調回路11でこの命令信号C1を受信すると、STEP3aにおいて、制御回路14でリーダー・ライタ1がメモリ領域18₁へのアクセスを希望していることを認識するとともに、図2のSTEP3と同様に、認証回路15に制御回路14で検知した認証信号Rc1を送出する。STEP4a及びSTEP5aにおいて、図2のSTEP4及びSTEP5と同様の動作を行う。

【0037】そして、制御回路14において、演算回路16で認証信号Rc1に基づいて生成された認証信号Rc2=f2(Rc1)及び、メモリ18より読み出した領域18₁の認識ID ID1aが、応答信号R1に付加される(STEP6a)。このように生成された応答信号R1は、変復調回路13で変調されて同調回路11よりリーダー・ライタ1に送信される(STEP7a)。

【0038】リーダー・ライタ1がこの応答信号R1を同調回路4より受信すると、STEP8a~14aにおいて、図2のSTEP8~14と同様の動作を行う。即ち、制御回路6で応答信号R1より認識ID ID1a及び認証信号Rc2を検知し、認証回路7によって認証信号Rc2に基づいて認証処理を行う。このとき、認証結果がNGの場合、コントローラ2との通信が行われずに、STEP10aに移行して演算回路で認証信号Rc3=f1(Rc2)を生成した後、認証信号Rc3を付加した命令信号C2'を生成する。又、認証結果がOKの場合、STEP11aに移行した後、コントローラ2でメモリ10内の認識ID ID1aに対応するメモリID ID1bを読み出してリーダー・ライタ1に送出し、認証信号Rc3及びメモリID ID1bを付加した命令信号C2を生成する。又、認識ID ID1aがメモリ10内に存在しないときは、上記した命令信号C2'が制御回路6で生成される。

【0039】このように、命令信号C2、C2'が生成されると、この命令信号をICカード31に送信する(STEP15a)。今、この認証信号Rc2=f2(Rc1)は演算f2()が施された信号であるので、リーダー・ライタ1はICカード31を認証する。よって、命令信号C2がICカード31に送信される。

【0040】ここで、STEP16a以降の動作については、図7で使用している記号以外は、図2のSTEP16以降の動作とほぼ同様であるので、以下、簡単に説明する。

【0041】今、ICカード31が命令信号C2を受信すると、制御回路14で、命令信号C2より認証信号Rc3及びメモリID ID1bを検知する(STEP16a)。尚、第1の実施形態と同様に、ICカード31が命令信号C2'を受信すると、リーダー・ライタ1、コントローラ2、及びICカード31においてSTEP3

a以降の動作を繰り返す。そして、認証回路15で認証信号Rc3がリーダー・ライタ1内で演算f1()が施された信号であるか否かを判別して、リーダー・ライタ1が適正か否かを判断する(STEP17a)。

【0042】このとき、認証結果がOKの場合、メモリ領域18₁のメモリIDと比較して、制御回路14にてリーダー・ライタ1から送信されたメモリIDが一致するか否かを判断し(STEP18a)、一致すればSTEP20aに移行し、一致しなければSTEP19aに移行する。又、STEP17aで認証結果がNGの場合、又は、STEP18aでメモリIDが不一致であるとき、制御回路14で検知された認証信号Rc3を演算回路16に送出し、演算回路16で認証信号Rc4=f2(Rc3)を生成して(STEP19a)、STEP20aに移行する。

【0043】STEP18a又はSTEP19aのような処理動作が終了しSTEP20aに移行すると、認証結果がOKのときは通信可能であることをリーダー・ライタ1に伝えるための応答信号R2を、認証結果がNGのときは認証信号Rc4及び認識ID ID1aを付加した応答信号R2'を制御回路14で生成した後、リーダー・ライタ1に送信する(STEP21a)。今、認証信号Rc3=f1(Rc2)で且つ、リーダー・ライタ1から送信されるメモリIDはID1bでありメモリ領域18₁のメモリIDと一致するので、STEP21aでは、通信可能であることをリーダー・ライタ1に伝えるための応答信号R2が送信される。

【0044】リーダー・ライタ1が応答信号R2を受信すると、制御回路6で、応答信号R2よりICカード31内のメモリ領域18₁が開放され、通信可能となったことを認識する(STEP22a)。尚、第1の実施形態と同様に、リーダー・ライタ1が応答信号R2'を受信すると、リーダー・ライタ1、コントローラ2、及びICカード31においてSTEP8a以降の動作を繰り返す。

【0045】今、応答信号R2を受信したものであるので、制御回路6よりコントローラ2の主制御回路9にICカード31と通信可能であることを認識させる(STEP23a)。コントローラ2がICカード31と通信可能であることを認識すると、リーダー・ライタ1を介してICカード31と相互に通信を行い、この通信を行う際にICカード31のメモリ領域18₁のデータの読み出し又は書き込みを行う(STEP24a)。

【0046】尚、第1及び第2の実施形態において、リーダー・ライタ、ICカードの間で複数回認証動作が行われ、全く認証が行われなかったとき、コントローラにエラーメッセージが送信され、通信が終了される。又、ICカード又はコントローラでID番号の確認が複数回行われ、いずれも不一致もしくは存在しないと判断されたとき、コントローラにエラーメッセージが送信され、通信が終了される。

【0047】本発明の第3の実施形態について、図面を参照して説明する。図10は、本実施形態における通信システムの構成を示すブロック図である。尚、本実施形態の通信システムにおいて、図10に示すリーダー・ライター及びコントローラの内部構造は、図1の通信システム内におけるリーダー・ライター及びコントローラ2の内部構造と同様のものとする。又、図10のICカードを構成するブロックにおいて、図1の通信システム内におけるICカード3を構成するブロックと同様のものは、同じ記号を付してその詳細な説明は省略する。

【0048】図10に示すICカード32は、領域19₁～19₃に分割されたメモリ19と、同調回路11と、整流回路12と、変復調回路13と、制御回路14と、認証回路15と、演算回路16とを有する。又、第1の実施形態におけるICカード3と同様、プロバイダC1、C2、C3がそれぞれ管理するリーダー・ライターと通信可能であり、メモリ19内において、プロバイダC1、C2、C3それぞれに、アクセスする領域19₁、19₂、19₃が振り分けられている。

【0049】又、プロバイダC1がICカード32を例えばその度数が金銭を表すプリペイドカードとして扱い、メモリ領域19₁内に、使用した度数毎にその度数を表すビット数が減少するようなダウンカウンタ（不図示）が構成されているものとする。更に、このダウンカウンタは、制御回路14からのリセット信号によって初期化される。今、プロバイダC1が管理するリーダー・ライター50にICカード32が近接して、第1又は第2の実施形態のような認証動作が行われ、リーダー・ライター50及びICカード32が相互認証した後、メモリ領域19₁が開放されて、コントローラ51とICカード32との間でリーダー・ライター50を介した通信が可能となったとする。

【0050】ICカード32のユーザーDが、例えばガソリンスタンドなどで代金を支払うために利用しているようなときの動作について説明する。まず、ダウンカウンタ内に保持されているビット数を読み出すための命令信号が、コントローラ51内のメモリ（不図示）に記憶しているユーザーDの残り度数の情報が付加され、この命令信号がコントローラ51よりリーダー・ライター50を介してICカード32に送信される。このとき、コントローラ51では、支払い後のユーザーDの残り度数を演算し主制御回路（不図示）内に記憶する。

【0051】ICカード32にこのような命令信号を受信すると、制御回路14よりダウンカウンタを読み出し可能とする信号がメモリ領域19₁に送出される。メモリ領域19₁に読み出し可能とする信号が送出されると、ダウンカウンタを読み出し可能とし、制御回路14でそのビット数がカウントされる。更に、制御回路14では、命令信号に付加されたコントローラ51内のメモリに記憶しているユーザーDの残り度数とダウンカウン

タから検知される度数とを比較して一致するか確認する。この度数が一致したとき、一致したことを知らせる応答信号を、リーダー・ライター50を介してコントローラ51に送信する。

【0052】コントローラ51は、この応答信号を受けると、リーダー・ライター50を介して、ダウンカウンタ内のビット数を代金分の度数に相当するビット数だけ減少させる命令信号をICカード32に送信する。このとき、コントローラ51では、支払い後のユーザーDの残り度数を演算し主制御回路（不図示）内に記憶する。ICカード32がこの命令信号を受けると、制御回路14よりダウンカウンタを書き込み可能とする信号がメモリ領域19₁に送出される。メモリ領域19₁に書き込み可能とする信号が送出されると、ダウンカウンタを書き込み可能とし、ダウンカウンタ内に保持されているビット数のうち、命令信号より検知されるビット数分削除される。

【0053】このように度数が削除されると、制御回路14で削除後のダウンカウンタのビット数が演算され、このビット数に相当する度数の情報が付加された応答信号が、リーダー・ライター50を介してコントローラ51に送信される。コントローラ51では、主制御回路に記憶した度数と応答信号より検知される度数を比較して一致したとき、一致したことを知らせる命令信号をICカード32に送信するとともに、コントローラ51のメモリにこの度数を記憶させて通信を終了する。

【0054】又、ICカード32とリーダー・ライター50が相互認証して通信可能となった後、度数を増加させるためにユーザーDが入金をしたときの動作を説明する。まず、ダウンカウンタ内に保持されているビット数を読み出すための命令信号に、コントローラ51内のメモリに記憶しているユーザーDの残り度数の情報が付加され、この命令信号がコントローラ51よりリーダー・ライター50を介してICカード32に送信される。

【0055】ICカード32にこのような命令信号を受信すると、制御回路14よりダウンカウンタを読み出し可能とする信号がメモリ領域19₁に送出される。メモリ領域19₁に読み出し可能とする信号が送出されると、ダウンカウンタを読み出し可能とし、制御回路14でそのビット数がカウントされる。更に、制御回路14では、命令信号に付加されたコントローラ51内のメモリに記憶しているユーザーDの残り度数とダウンカウンタから検知される度数とを比較して一致するか確認する。この度数が一致したとき、一致したことを知らせる応答信号を、リーダー・ライター50を介してコントローラ51に送信する。

【0056】コントローラ51は、この応答信号を受けると、リーダー・ライター50を介して、ダウンカウンタ内のビット数を入金後の度数に相当するビット数に変更させる命令信号をICカード32に送信する。このとき、

コントローラ51では、入金後のユーザーDの残り度数を演算し主制御回路内に記憶する。ICカード32がこの命令信号を受けると、制御回路14よりダウンカウンタを書き込み可能とする信号がメモリ領域19₁に送出される。メモリ領域19₁に書き込み可能とする信号が送出されると、ダウンカウンタを書き込み可能となる。その後、制御回路14よりリセット信号が送信され、一旦、初期化される。このように初期化された後、ダウンカウンタ内に保持されているビット数が命令信号より検知されるビット数に相当するまで削除される。

【0057】このように度数が変更されると、制御回路14で変更後のダウンカウンタのビット数が演算され、このダウンカウンタのビット数に相当する度数の情報が付加された応答信号が、リーダ・ライタ50を介してコントローラ51に送信される。コントローラ51では、主制御回路に記憶した度数と応答信号より検知される度数を比較して一致したとき、一致したことを知らせる命令信号をICカードに送信するとともに、コントローラ51のメモリにこの度数を記憶させて通信を終了する。

【0058】以上の実施形態では、ICカードといった非接触で通信を行う通信用応答器を用いて説明したが、このような応答器に限らず、接触して通信を行うような通信用応答器でも良い。尚、接触して通信を行う場合、第1～第3の実施形態のように信号の送受信を行うための同調回路を用いる代わりに、入出力インターフェイスを応答器及び質問器に設けることによって、その通信が可能となる。

【0059】

【発明の効果】請求項1に記載の通信用応答器は、記憶領域を使用可能にするための鍵信号を、該応答器固有の鍵信号として設定し、この鍵信号によって前記憶領域の使用を許可するような構成となっているので、この通信用応答器を使用することで、より安全性の高い通信システムを形成することができる。

【0060】請求項2に記載の通信用応答器は、前記質問器に通信の許可を求めるための信号を生成する認証手段が設けられているので、質問器が応答器の認証を行うまで、通信が行われないので、この通信用応答器を使用することで、請求項1に記載の通信用応答器より安全性の高い通信システムを形成することができる。

【0061】請求項3に記載の通信用応答器は、質問器から通信の許可を求めてきた信号を検知し、該信号によって質問器が適正なものか否かを判別する認証手段が設けられているので、応答器が質問器の認証を行うまで、通信が行われないので、この通信用応答器を使用することで、請求項1に記載の通信用応答器より安全性の高い通信システムを形成することができる。

【0062】請求項4に記載の通信用応答器は、前記質問器に通信の許可を求めるための信号を生成する演算手段と、質問器から通信の許可を求めてきた信号を検知

し、該信号によって質問器が適正なものか否かを判別する認証手段とが設けられているので、この通信用応答器を使用することで、請求項1に記載の通信用応答器より安全性の高い通信システムを形成することができる。

【0063】請求項5に記載の通信用応答器は、少なくとも1つの記憶領域が度数記憶部材によって構成されるので、プリペイドカードのような、その度数を金銭の代わりとして用いることを目的とした記憶領域を形成することが可能となる。

【0064】請求項6に記載の非接触通信システムは、請求項1～5のいずれかに記載の通信用応答器を使用した通信システムであるので、質問器及び応答器の双方が認証するために、応答器固有の鍵信号が用いられ、安全性の高い通信システムとして構成される。

【図面の簡単な説明】

【図1】本発明の第1の実施形態で使用する通信システムの構成を示すブロック図。

【図2】図1に示す通信システムの動作を示すタイムチャート。

【図3】図1に示す通信システムにおいてリーダ・ライタを管理するプロバイダとICカード内のメモリ領域の関係を示すブロック図。

【図4】図1に示す通信システムで使用するICカードの個々の関係を示すブロック図。

【図5】図1に示す通信システムで使用するコントローラの内部及びメモリ内部の構造を示すブロック図。

【図6】本発明の第2の実施形態で使用する通信システムの構成を示すブロック図。

【図7】図6に示す通信システムの動作を示すタイムチャート。

【図8】図6に示す通信システムで使用するICカードの個々の関係を示すブロック図。

【図9】図6に示す通信システムで使用するコントローラの内部及びメモリ内部の構造を示すブロック図。

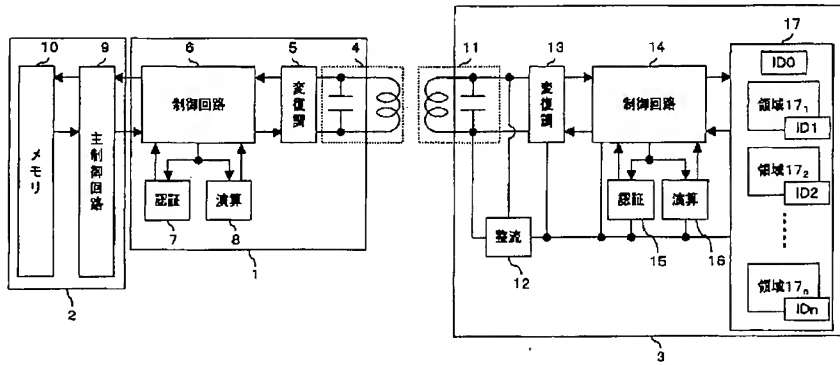
【図10】本発明の第3の実施形態で使用する通信システムの構成を示すブロック図。

【図11】従来の通信システムの構成を示すブロック図。

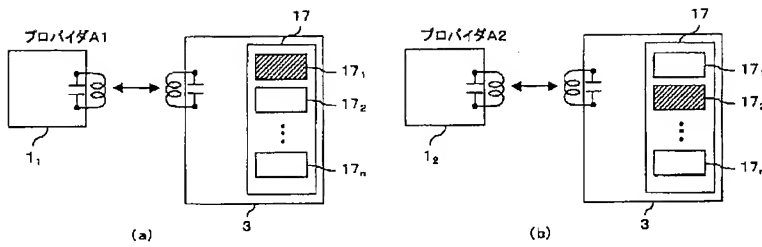
【符号の説明】

- 1, 50 リーダ・ライタ
- 2, 51 コントローラ
- 3, 31, 32 ICカード
- 4, 11 同調回路
- 5, 13 変復調回路
- 6, 14 制御回路
- 7, 15 認証回路
- 8, 16 演算回路
- 9 主制御回路
- 10, 17, 18, 19 メモリ
- 12 整流回路

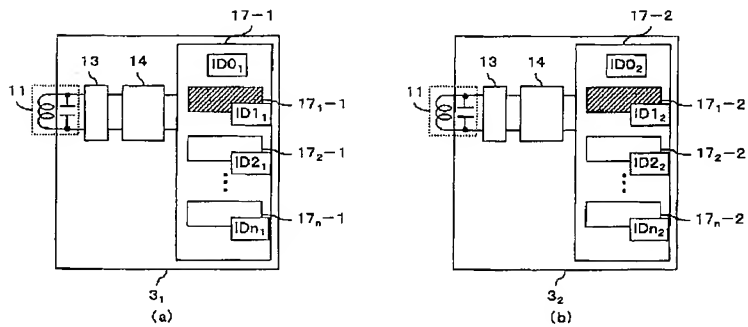
【図1】



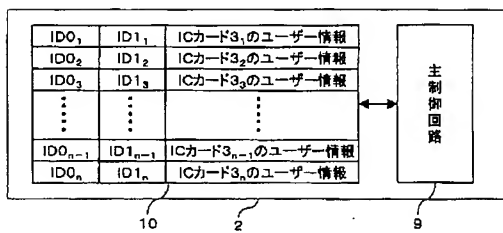
【図3】



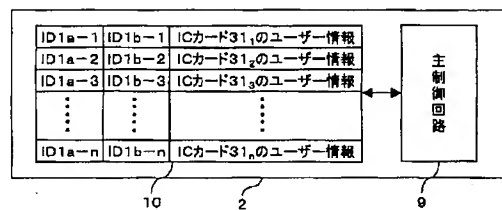
【図4】



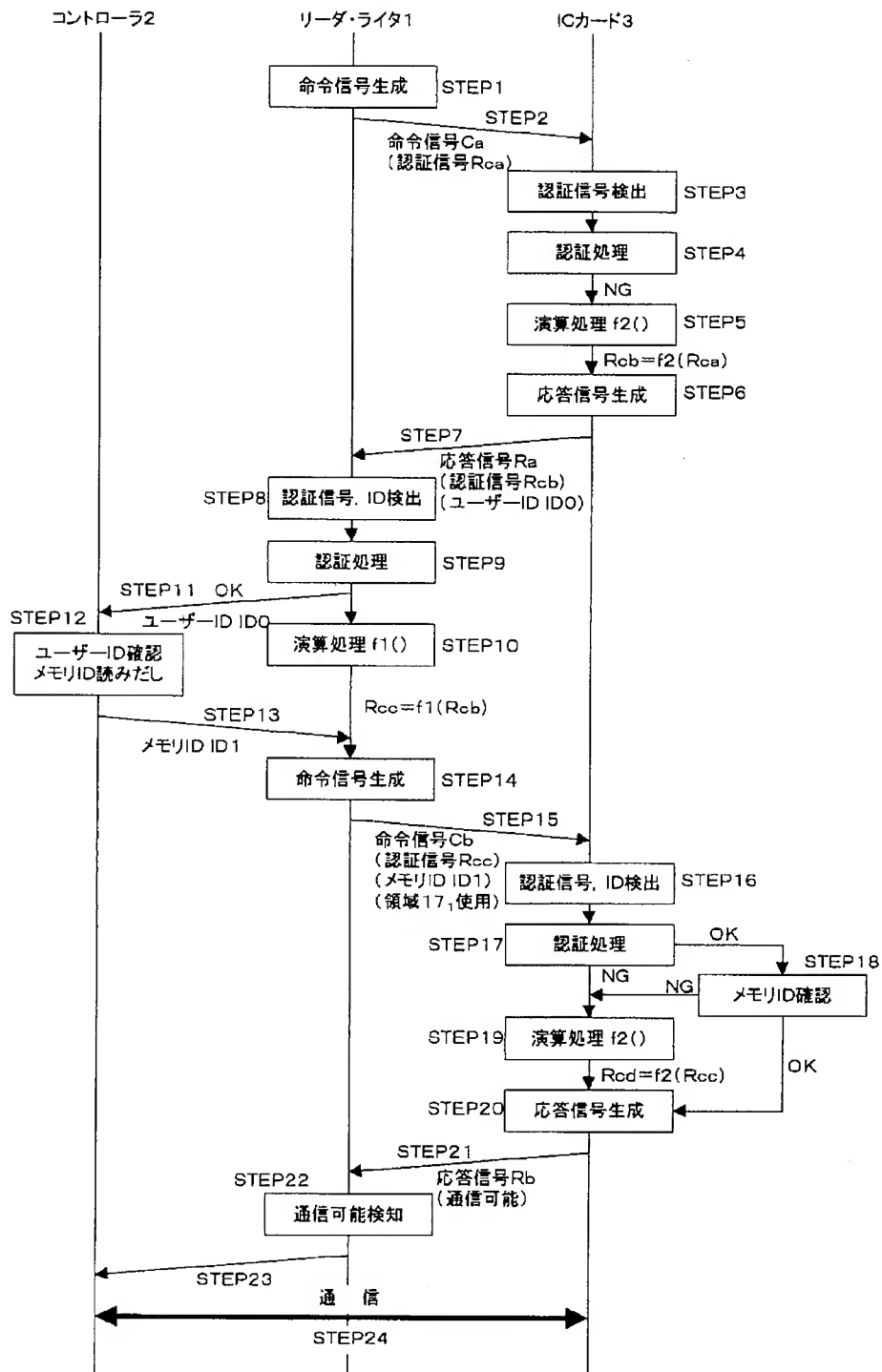
【図5】



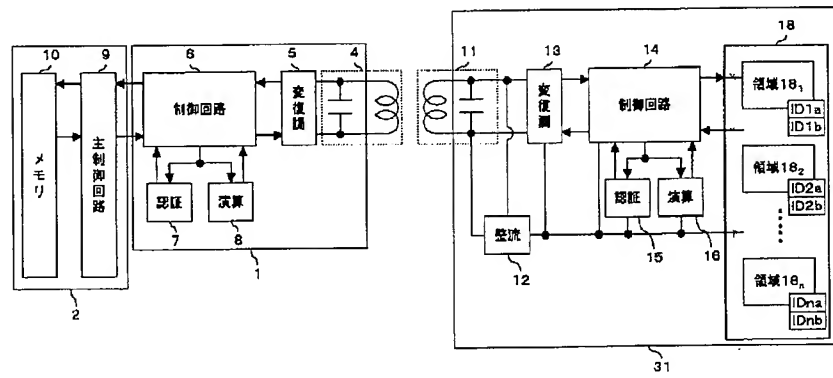
【図9】



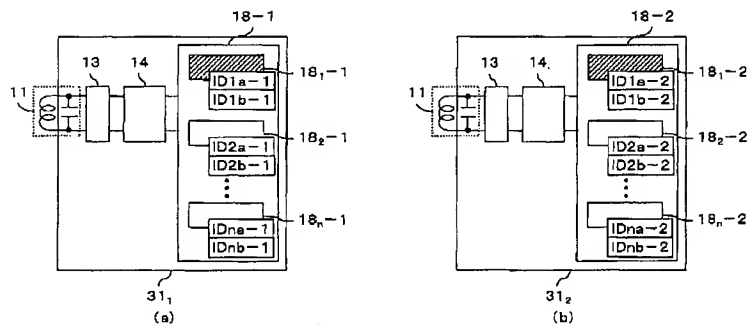
【図2】



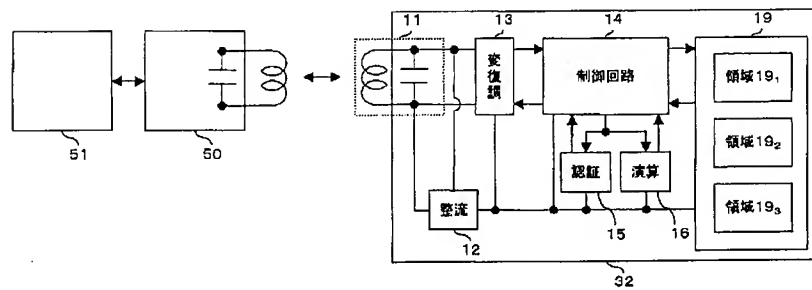
【図6】



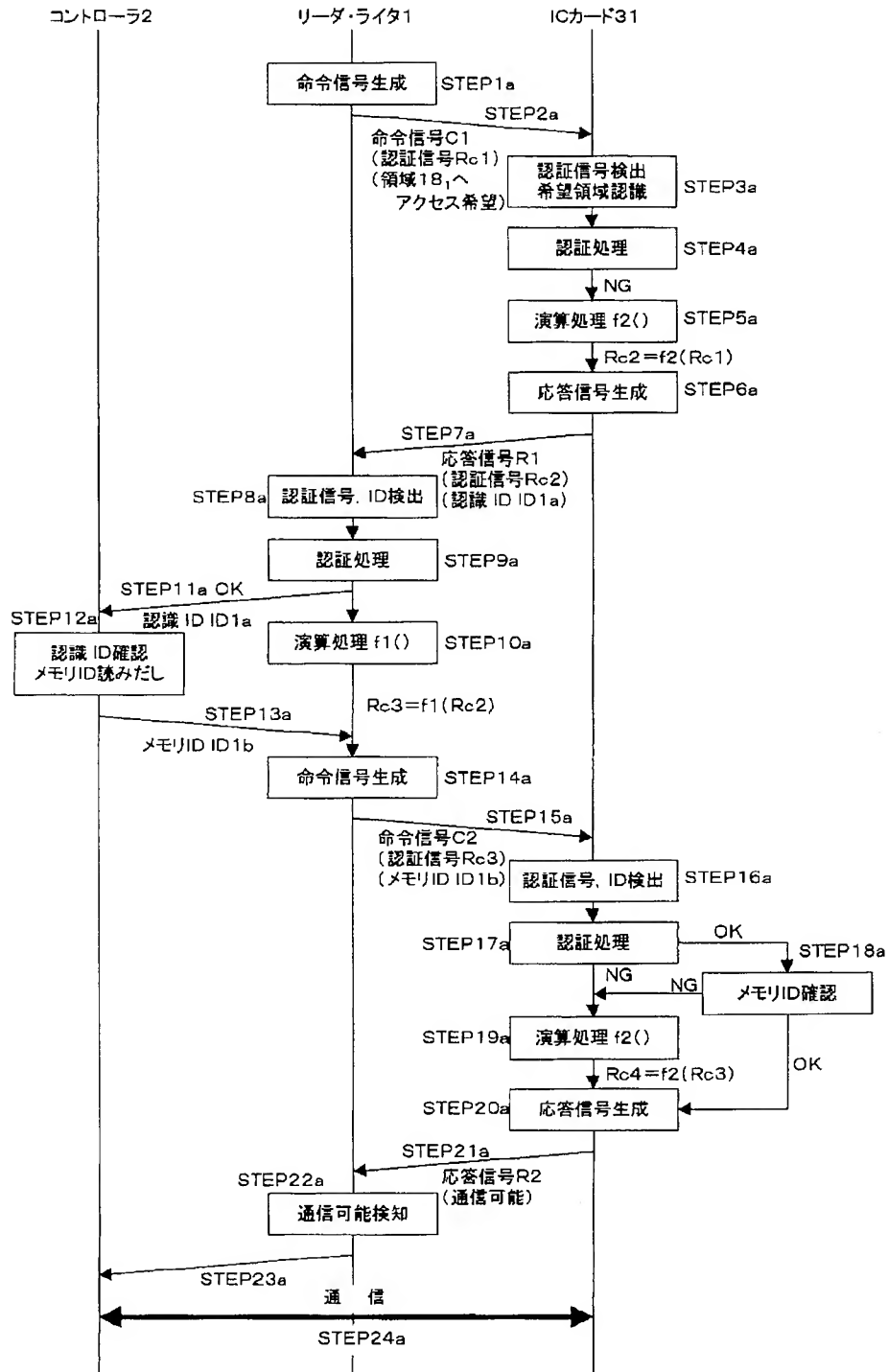
【図8】



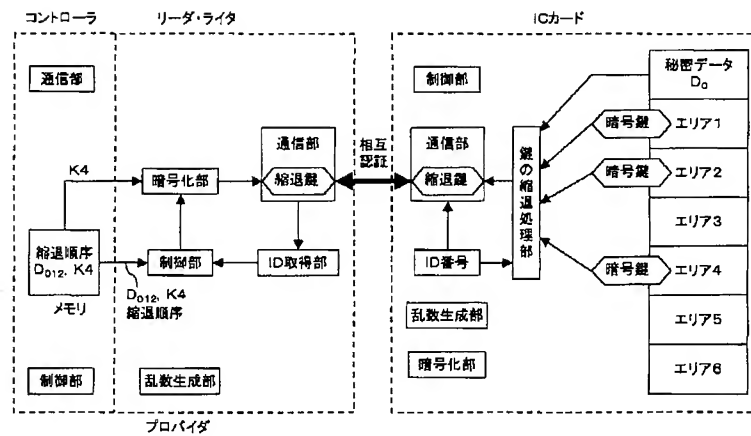
【図10】



【図7】



【図11】



フロントページの続き

(72)発明者 田口 治生
京都市右京区西院溝崎町21番地 ローム株
式会社内

F ターム(参考) 5B058 CA15 CA27 KA33 KA40
5J104 AA07 KA02 KA04 NA02 NA35
NA36 NA38 PA00
5K012 AB03 AC09 AC11 BA07
9A001 CC05 EE03 HH34 JJ66 KK57
LL03